

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-350678

(P2001-350678A)

(43)公開日 平成13年12月21日(2001.12.21)

(51) Int.Cl.⁷

識別記号

FI

テーマコード* (参考)

G O 6 F 13/00

3 5 1

G O 6 F 13/00

3 5 1 Z 5 B 0 8 9

H 0 4 L 12/22

H04L 11/26

5 K 0 3 0

審査請求 未請求 請求項の数13 O.L (全 19 頁)

(21)出願番号 特願2000-170727(P2000-170727)

(22) 出題日 平成12年6月7日(2000.6.7)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 小林 信博

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74) 代理人 100099461

弁理士 溝井 章司 (外2名)

Fターム(参考) 5B089 GA11 GA21 GB02 KA17 KB13

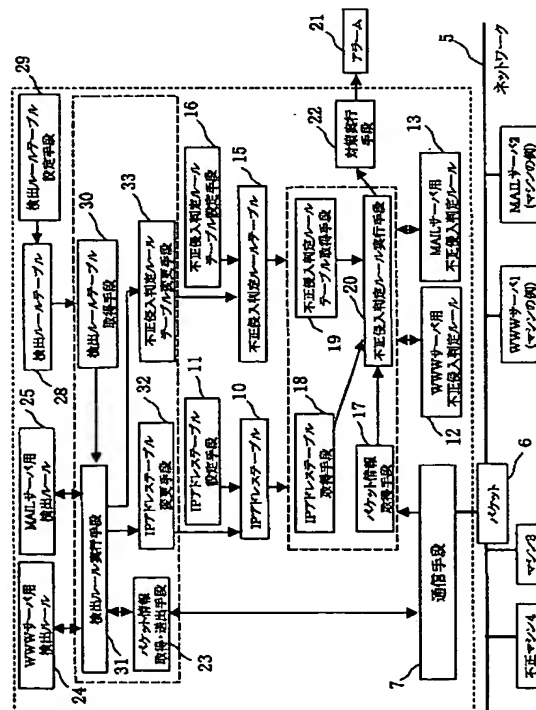
5K030 GA15 GA17 HA08 HB28

(54)【発明の名称】 不正侵入検知システム

(57) 【要約】

【課題】 I P アドレステーブルと不正侵入判定ルールテーブルを用いて、不正侵入判定を行なう不正侵入検知システムに係り、I P アドレステーブルと不正侵入判定ルールテーブルの設定変更を自動的に行う不正侵入検知システムを提供することを課題とする。

【解決手段】 検出ルール実行手段 3 1 の動作結果に基づいて、IP アドレステーブル変更手段 3 2 が、IP アドレステーブル 1 0 を変更し、不正侵入判定ルールテーブル変更手段 3 3 が、不正侵入判定ルールテーブル 1 5 を変更し、これらのテーブルを用いて、不正侵入判定ルール実行手段 2 0 は、不正侵入の判定を行なう。



【特許請求の範囲】

【請求項 1】 ネットワークを介してマシンに接続し、マシンに対する不正侵入を検知する不正侵入検知システムであって、以下の要素を有することを特徴とする不正侵入検知システム (1) ネットワークに接続するマシンの識別情報と、マシンの IP アドレスとを対応付けて記憶する IP アドレステーブル、(2) ネットワークに接続するマシンの識別情報と、マシンに対する不正侵入を判定する不正侵入判定ルールの識別情報とを対応付けて記憶する不正侵入判定ルールテーブル、(3) ネットワークを介してパケットの送受信を行なう通信手段、

(4) 通信手段からパケットを取得し、取得したパケットに含まれる IP アドレスを取り出すパケット情報取得手段、(5) IP アドレステーブルから、パケット情報取得手段により取り出した IP アドレスと一致する IP アドレスに対応するマシンの識別情報を選択し、不正侵入判定ルールテーブルから、選択したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を選択し、

選択した識別情報で識別される不正侵入判定ルールに従って、不正侵入を判定する不正侵入判定ルール実行手段、(6) 通信手段からパケットを取得し、

取得したパケットに含まれる IP アドレスを取り出し、取り出した IP アドレスで特定されるマシンに対して接続し、

接続したマシン上で動作しているサーバの種類を取得し、

取得したサーバの種類に適した不正侵入判定ルールを選択し、

接続したマシンの識別情報を生成する検出ルール実行手段、

(7) 検出ルール実行手段により生成したマシンの識別情報と、取り出した IP アドレスとを対応付けて、IP アドレステーブルに記憶させる IP アドレステーブル変更手段、(8) 検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させる不正侵入判定ルールテーブル変更手段。

【請求項 2】 不正侵入検知システムは、更に、サーバの種類と、そのサーバの種類に適した不正侵入判定ルールの識別情報とを対応付けて記憶する検出ルールテーブルを有し、

検出ルール実行手段は、検出ルールテーブルで、サーバの種類に対応つけられる不正侵入判定ルールの識別情報を出力することを特徴とする請求項 1 記載の不正侵入検知システム。

【請求項 3】 不正侵入検知システムは、更に、IP アドレステーブルに、検出ルール実行手段により取り出した IP アドレスと一致する IP アドレスが記憶されているかを検査する IP アドレス設定済検査手段を有し、

IP アドレステーブル変更手段は、IP アドレス設定済検査手段により、一致する IP アドレスが記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、取り出した IP アドレスとを対応付けて、IP アドレステーブルに記憶させることを特徴とする請求項 1 記載の不正侵入検知システム。

【請求項 4】 不正侵入検知システムは、更に、不正侵入判定ルールテーブルに、検出ルール実行手段により選択した不正侵入判定ルールの識別情報と一致する識別情報が記憶されているかを検査する不正侵入判定ルール設定済検査手段を有し、

不正侵入判定ルールテーブル変更手段は、不正侵入判定ルール設定済検査手段により、一致する不正侵入判定ルールの識別情報が記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させることを特徴とする請求項 1 記載の不正侵入検知システム。

【請求項 5】 不正侵入検知システムは、更に、IP アドレステーブルから、マシンの識別情報と、マシンの IP アドレスとを取得する IP アドレステーブル再取得手段と、

不正侵入判定ルールテーブルから、IP アドレステーブル再取得手段により取得したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を取得する不正侵入判定ルールテーブル再取得手段と、

検出ルール実行手段に、IP アドレステーブル再取得手段により取得した IP アドレスで特定されるマシンに接続させ、接続したマシン上で動作しているサーバの種類を取得させる検出ルール再実行手段とを有し、

不正侵入判定ルールテーブル変更手段は、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報により識別される不正侵入識別ルールが適するサーバの種類と、ルール実行手段により取得したサーバの種類とが一致しない場合に、

不正侵入判定ルールテーブルから、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報を削除することを特徴とする請求項 1 記載の不正侵入検知システム。

【請求項 6】 不正侵入検知システムは、更に、IP アドレステーブルから、マシンの識別情報と、マシンの IP アドレスとを取得する IP アドレステーブル再取得手段と、

検出ルール実行手段に、IP アドレステーブル再取得手段により取得した IP アドレスで特定されるマシンに接続させる検出ルール再実行手段とを有し、

IP アドレステーブル変更手段は、検出ルール実行手段による接続ができない場合に、IP アドレステーブルから、IP アドレステーブル再取得手段により取得したマシンの識別情報と、マシンの IP アドレスとを削除し、

3

不正侵入判定ルールテーブル変更手段は、IPアドレステーブル再取得手段により取得したマシンの識別情報と、その識別情報に対応する不正侵入判定ルールの識別情報とを削除することを特徴とする請求項1記載の不正侵入検知システム。

【請求項7】 不正侵入検知システムは、更に、不正侵入判定ルール手段により不正侵入があったことを判定した場合に、対策としてアラームを出力する対策実行手段と、

対策実行手段により出力されたアラームを検知するアラーム検出手段と、

アラーム検出手段によりアラームを検出した場合に、検出ルール再実行手段を起動する再検出指定手段とを有することを特徴とする請求項5または6記載の不正侵入検知システム。

【請求項8】 不正侵入検知システムは、更に、検出ルールテーブルを暗号化する検出ルールテーブル暗号設定手段と、

暗号化した検出ルールテーブルを復号する検出ルールテーブル復号取得手段と、

IPアドレステーブルを暗号化するIPアドレステーブル暗号設定手段と、

暗号化したIPアドレステーブルを復号するIPアドレステーブル復号取得手段と、

不正侵入判定ルールテーブルを暗号化する不正侵入判定ルールテーブル暗号設定手段と、

暗号化した不正侵入判定ルールテーブルを復号する不正侵入判定ルールテーブル復号取得手段とを有することを特徴とする請求項2記載の不正侵入検知システム。

【請求項9】 不正侵入検知システムは、更に、検出ルールテーブルと、IPアドレステーブルと、不正侵入判定テーブルとの変更履歴を生成するテーブル変更保存手段と、

テーブル変更保存手段により生成した変更履歴を格納する履歴テーブルとを有することを特徴とする請求項1記載の不正侵入検知システム。

【請求項10】 不正侵入検知システムは、更に、通信手段からパケットを取得して保存するパケット保存手段と、

パケット保存手段に保存したパケット出力するパケット再生手段とを有し、

検出ルール実行手段は、パケット再生手段により出力されるパケットを取得することを特徴とする請求項1記載の不正侵入検知システム。

【請求項11】 不正侵入検知システムは、更に、パケット再生手段がパケットを出力するスケジュールを記憶する再生スケジュール記憶部と、

再生スケジュール記憶部に記憶するスケジュールに従って、パケット再生手段へパケットの出力を指示する指定日時パケット再生指示手段とを有することを特徴とする

4

請求項10記載の不正侵入検知システム。

【請求項12】 不正侵入検知システムは、更に、システムの負荷状況を取得する負荷取得手段と、

負荷取得手段により取得した負荷状況が、所定の負荷よりも小さいと判断した場合に、パケット再生手段へパケットの出力を指示する低負荷時パケット再生指示手段とを有することを特徴とする請求項10記載の不正侵入検知システム。

【請求項13】 不正侵入検知システムは、更に、パケット保存手段からパケットの流通量を取得するパケット流通量取得手段と、

パケット流通量取得手段により取得したパケットの流通量が、所定の流通量よりも少ないと判断した場合に、パケット再生手段へパケットの出力を指示する低ネットワーク負荷時パケット再生指示手段とを有することを特徴とする請求項10記載の不正侵入検知システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ネットワーク上を流れるパケットを入手して動作する不正侵入検知システムの設定方法に関する。

【0002】

【従来の技術】図17は、例えばコンピュータ・セキュリティ・シンポジウム'99にて発表された「パケット監視によるネットワーク侵入検出システムの実装と評価」に代表されるような従来の侵入検知システムである。

【0003】ネットワーク5は、WWWサーバ1、MAILサーバ2、正常マシン3、不正マシン4などを接続している。ネットワーク5上には、データ転送の為にパケット6が流れている。

【0004】そのため、不正侵入検知システムは、通信手段7、IPアドレステーブル10、IPアドレステーブル設定手段11、WWWサーバ用不正侵入判定ルール12、MAILサーバ用不正侵入判定ルール13、不正侵入判定ルールテーブル15、不正侵入判定ルールテーブル設定手段16、パケット情報取得手段17、IPアドレステーブル取得手段18、不正侵入判定ルールテーブル取得手段19、不正侵入判定ルール実行手段20、対策実行手段22を備えている。

【0005】通信手段7は、ネットワーク5とパケット6のやりとりを行う。

【0006】IPアドレステーブル10は、マシン名8とIPアドレス9の関係をまとめたIPアドレスリストを記述している。尚、マシン名8は、WWWサーバ1、MAILサーバ2、正常マシン3や不正マシン4などを識別する。また、IPアドレス9は、WWWサーバ1やMAILサーバ2や正常マシン3や不正マシン4などが送受するパケット6の中に含まれるIPアドレスである。

10

20

30

40

50

【0007】IPアドレステーブル設定手段11は、IPアドレステーブル10を設定する。

【0008】WWWサーバ用不正侵入判定ルール12は、パケット6の情報をもとにWWWサーバに対する不正侵入を判定するルールである。

【0009】MAILサーバ用不正侵入判定ルール13は、パケット6の情報をもとにMAILサーバに対する不正侵入を判定するルールである。

【0010】不正侵入判定ルールテーブル15は、マシン名8と不正侵入判定ルール名14の関係をまとめた不正侵入判定ルールリストを記述している。尚、不正侵入判定ルール名14は、WWWサーバ用不正侵入判定ルール12やMAILサーバ用不正侵入判定ルール13などを識別するルール名である。

【0011】不正侵入判定ルールテーブル設定手段16は、不正侵入判定ルールテーブル15を設定する。

【0012】パケット情報取得手段17は、通信手段7からパケット6を取得する。

【0013】IPアドレステーブル取得手段18は、IPアドレステーブル10からIPアドレスリストを取得する。

【0014】不正侵入判定ルールテーブル取得手段19は、不正侵入判定ルールテーブル15から不正侵入判定ルールリストを取得する。

【0015】不正侵入判定ルール実行手段20は、IPアドレスリストから、パケット6から取り出したIPアドレス9に対応するマシン名8を特定し、不正侵入判定ルールテーブルリストからそのマシン名8に対応する不正侵入判定ルールを特定し、その不正侵入判定ルールを実行する。

【0016】対策実行手段22は、不正侵入判定ルール実行手段20の結果に応じて、アラーム出力などの制御を行なう。これにより、不正侵入判定ルール実行結果が不正侵入と判定されたときにアラームが出力する。

【0017】このような従来の侵入検知システムにおいては、パケット情報取得手段17により通信手段7から得られたパケット6を利用し、IPアドレステーブル設定手段11によってユーザーから設定されたIPアドレステーブル10と、不正侵入判定ルールテーブル設定手段16によってユーザーから設定された不正侵入判定ルールテーブル15に基づき、不正侵入判定ルール実行手段20が該当する不正侵入判定ルールを呼び出して侵入検知を行う。

【0018】従来の侵入検知システムにおいては、ユーザーが手作業によりIPアドレステーブル10と不正侵入判定ルールテーブル15を設定していた為、煩雑であるという欠点があった。

【0019】また、マシンが追加された場合にユーザーが再設定しなくてはならないという欠点があった。

【0020】また、マシン上で新たなサーバが実行され

るようになった場合にユーザーが再設定しなくてはならないという欠点があった。

【0021】また、設定時にユーザーが操作ミスをして意図しない設定のまま実行されるという問題もあった。

【0022】

【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、IPアドレステーブルと不正侵入判定ルールテーブルの設定変更を自動的に行うものである。

【0023】また、マシンが追加された場合に自動的にIPアドレステーブルを変更する。

【0024】また、そのマシン上で稼働しているサーバを自動的に判定し、不正侵入判定ルールテーブルを変更する。

【0025】また、マシン上で新たなサービスが稼働した場合に自動的に不正侵入判定ルールテーブルを変更する。

【0026】

【課題を解決するための手段】この発明に係る不正侵入検知システムは、ネットワークを介してマシンに接続し、マシンに対する不正侵入を検知する不正侵入検知システムであって、以下の要素を有することを特徴とする。

(1) ネットワークに接続するマシンの識別情報と、マシンのIPアドレスとを対応つけて記憶するIPアドレステーブル、(2) ネットワークに接続するマシンの識別情報と、マシンに対する不正侵入を判定する不正侵入判定ルールの識別情報とを対応付けて記憶する不正侵入判定ルールテーブル、(3) ネットワークを介してパケットの送受信を行なう通信手段、(4) 通信手段からパケットを取得し、取得したパケットに含まれるIPアドレスを取り出すパケット情報取得手段、(5) IPアドレステーブルから、パケット情報取得手段により取り出したIPアドレスと一致するIPアドレスに対応するマシンの識別情報を選択し、不正侵入判定ルールテーブルから、選択したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を選択し、選択した識別情報で識別される不正侵入判定ルールに従って、不正侵入を判定する不正侵入判定ルール実行手段、

(6) 通信手段からパケットを取得し、取得したパケットに含まれるIPアドレスを取り出し、取り出したIPアドレスで特定されるマシンに対して接続し、接続したマシン上で動作しているサーバの種類を取得し、取得したサーバの種類に適した不正侵入判定ルールを選択し、接続したマシンの識別情報を生成する検出ルール実行手段、(7) 検出ルール実行手段により生成したマシンの識別情報と、取り出したIPアドレスとを対応つけて、IPアドレステーブルに記憶させるIPアドレステーブル変更手段、(8) 検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識

10

20

30

40

50

別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させる不正侵入判定ルールテーブル変更手段。

【0027】また、不正侵入検知システムは、更に、サーバの種類と、そのサーバの種類に適した不正侵入判定ルールの識別情報とを対応付けて記憶する検出ルールテーブルを有し、検出ルール実行手段は、検出ルールテーブルで、サーバの種類に対応つけられる不正侵入判定ルールの識別情報を出力することを特徴とする。

【0028】また、不正侵入検知システムは、更に、IPアドレステーブルに、検出ルール実行手段により取り出したIPアドレスと一致するIPアドレスが記憶されているかを検査するIPアドレス設定済検査手段を有し、IPアドレステーブル変更手段は、IPアドレス設定済検査手段により、一致するIPアドレスが記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、取り出したIPアドレスとを対応付けて、IPアドレステーブルに記憶させることを特徴とする。

【0029】また、不正侵入検知システムは、更に、不正侵入判定ルールテーブルに、検出ルール実行手段により選択した不正侵入判定ルールの識別情報と一致する識別情報が記憶されているかを検査する不正侵入判定ルール設定済検査手段を有し、不正侵入判定ルールテーブル変更手段は、不正侵入判定ルール設定済検査手段により、一致する不正侵入判定ルールの識別情報が記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させることを特徴とする。

【0030】また、不正侵入検知システムは、更に、IPアドレステーブルから、マシンの識別情報と、マシンのIPアドレスとを取得するIPアドレステーブル再取得手段と、不正侵入判定ルールテーブルから、IPアドレステーブル再取得手段により取得したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を取得する不正侵入判定ルールテーブル再取得手段と、検出ルール実行手段に、IPアドレステーブル再取得手段により取得したIPアドレスで特定されるマシンに接続させ、接続したマシン上で動作しているサーバの種類を取得させる検出ルール再実行手段とを有し、不正侵入判定ルールテーブル変更手段は、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報により識別される不正侵入識別ルールが適するサーバの種類と、ルール実行手段により取得したサーバの種類とが一致しない場合に、不正侵入判定ルールテーブルから、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報を削除することを特徴とする。

【0031】また、不正侵入検知システムは、更に、IPアドレステーブルから、マシンの識別情報と、マシン

のIPアドレスとを取得するIPアドレステーブル再取得手段と、検出ルール実行手段に、IPアドレステーブル再取得手段により取得したIPアドレスで特定されるマシンに接続させる検出ルール再実行手段とを有し、IPアドレステーブル変更手段は、検出ルール実行手段による接続ができない場合に、IPアドレステーブルから、IPアドレステーブル再取得手段により取得したマシンの識別情報と、マシンのIPアドレスとを削除し、不正侵入判定ルールテーブル変更手段は、IPアドレステーブル再取得手段により取得したマシンの識別情報と、その識別情報に対応する不正侵入判定ルールの識別情報を削除することを特徴とする。

【0032】また、不正侵入検知システムは、更に、不正侵入判定ルール手段により不正侵入があったことを判定した場合に、対策としてアラームを出力する対策実行手段と、対策実行手段により出力されたアラームを検知するアラーム検出手段と、アラーム検出手段によりアラームを検出した場合に、検出ルール再実行手段を起動する再検出指定手段とを有することを特徴とする。

【0033】また、不正侵入検知システムは、更に、検出ルールテーブルを暗号化する検出ルールテーブル暗号設定手段と、暗号化した検出ルールテーブルを復号する検出ルールテーブル復号取得手段と、IPアドレステーブルを暗号化するIPアドレステーブル暗号設定手段と、暗号化したIPアドレステーブルを復号するIPアドレステーブル復号取得手段と、不正侵入判定ルールテーブルを暗号化する不正侵入判定ルールテーブル暗号設定手段と、暗号化した不正侵入判定ルールテーブルを復号する不正侵入判定ルールテーブル復号取得手段とを有することを特徴とする。

【0034】また、不正侵入検知システムは、更に、検出ルールテーブルと、IPアドレステーブルと、不正侵入判定テーブルとの変更履歴を生成するテーブル変更保存手段と、テーブル変更保存手段により生成した変更履歴を格納する履歴テーブルとを有することを特徴とする。

【0035】また、不正侵入検知システムは、更に、通信手段からパケットを取得して保存するパケット保存手段と、パケット保存手段に保存したパケット出力するパケット再生手段とを有し、検出ルール実行手段は、パケット再生手段により出力されるパケットを取得することを特徴とする。

【0036】また、不正侵入検知システムは、更に、パケット再生手段がパケットを出力するスケジュールを記憶する再生スケジュール記憶部と、再生スケジュール記憶部に記憶するスケジュールに従って、パケット再生手段へパケットの出力を指示する指定日時パケット再生指示手段とを有することを特徴とする。

【0037】また、不正侵入検知システムは、更に、システムの負荷状況を取得する負荷取得手段と、負荷取得

10

20

30

40

50

手段により取得した負荷状況が、所定の負荷よりも小さいと判断した場合に、パケット再生手段へパケットの出力を指示する低負荷時パケット再生指示手段とを有することを特徴とする。

【0038】また、不正侵入検知システムは、更に、パケット保存手段からパケットの流通量を取得するパケット流通量取得手段と、パケット流通量取得手段により取得したパケットの流通量が、所定の流通量よりも少ないと判断した場合に、パケット再生手段へパケットの出力を指示する低ネットワーク負荷時パケット再生指示手段とを有することを特徴とする。

【0039】

【発明の実施の形態】実施の形態 1. 以下本発明を図面に示す実施例に基づいて説明する。図 1 は、実施の形態 1 における侵入検知システムを示す図である。ネットワーク 5 は、WWWサーバ 1、MAILサーバ 2、正常マシン 3、不正マシン 4 などを接続している。ネットワーク 5 上には、データ転送の為にパケット 6 が流れている。

【0040】そのため、不正侵入検知システムは、通信手段 7、IP アドレステーブル 10、IP アドレステーブル設定手段 11、WWWサーバ用不正侵入判定ルール 12、MAILサーバ用不正侵入判定ルール 13、不正侵入判定ルールテーブル 15、不正侵入判定ルールテーブル設定手段 16、パケット情報取得手段 17、IP アドレステーブル取得手段 18、不正侵入判定ルールテーブル取得手段 19、不正侵入判定ルール実行手段 20、対策実行手段 22、パケット情報取得・送出手段 23、WWWサーバ用検出ルール 24、MAILサーバ用検出ルール 25、検出ルールテーブル 28、検出ルールテーブル設定手段 29、検出ルールテーブル取得手段 30、検出ルール実行手段 31、IP アドレステーブル変更手段 32、不正侵入判定ルールテーブル変更手段 33 を備える。

【0041】通信手段 7 は、ネットワーク 5 とパケット 6 のやりとりを行う。

【0042】IP アドレステーブル 10 は、マシン名 8 と IP アドレス 9 の関係をまとめた IP アドレスリストを記述している。図 2 は、IP アドレステーブルの構成を示す図である。尚、マシン名 8 は、WWWサーバ 1、MAILサーバ 2、正常マシン 3 や不正マシン 4 などを識別する。また、IP アドレス 9 は、WWWサーバ 1 や MAILサーバ 2 や正常マシン 3 や不正マシン 4 などが送受するパケット 6 の中に含まれる IP アドレスである。

【0043】IP アドレステーブル設定手段 11 は、IP アドレステーブル 10 を設定する。

【0044】WWWサーバ用不正侵入判定ルール 12 は、パケット 6 の情報をもとに WWWサーバに対する不正侵入を判定するルールである。

【0045】MAILサーバ用不正侵入判定ルール 13 は、パケット 6 の情報をもとに MAILサーバに対する不正侵入を判定するルールである。

【0046】不正侵入判定ルールテーブル 15 は、マシン名 8 と不正侵入判定ルール名 14 の関係をまとめた不正侵入判定ルールリストを記述している。図 3 は、ルールテーブルの構成を示す図である。尚、不正侵入判定ルール名 14 は、WWWサーバ用不正侵入判定ルール 12 や MAILサーバ用不正侵入判定ルール 13 などを識別するルール名である。

【0047】不正侵入判定ルールテーブル設定手段 16 は、不正侵入判定ルールテーブル 15 を設定する。

【0048】パケット情報取得手段 17 は、通信手段 7 からパケット 6 を取得する。

【0049】IP アドレステーブル取得手段 18 は、IP アドレステーブル 10 から IP アドレスリストを取得する。

【0050】不正侵入判定ルールテーブル取得手段 19 は、不正侵入判定ルールテーブル 15 から不正侵入判定ルールリストを取得する。

【0051】不正侵入判定ルール実行手段 20 は、IP アドレスリストから、パケット 6 から取り出した IP アドレス 9 に対応するマシン名 8 を特定し、不正侵入判定ルールテーブルリストからそのマシン名 8 に対応する不正侵入判定ルールを特定し、その不正侵入判定ルールを実行する。

【0052】対策実行手段 22 は、不正侵入判定ルール実行手段 20 の結果に応じて、アラーム出力などの制御を行なう。これにより、不正侵入判定ルール実行結果が不正侵入と判定されたときにアラーム 21 が出力する。

【0053】パケット情報取得・送出手段 23 は、通信手段 7 からパケット 6 を取得または送出する。

【0054】WWWサーバ用検出ルール 24 は、パケット 6 の情報をもとに WWWサーバ 1 かどうかの検出を行うルールである。

【0055】MAILサーバ用検出ルール 25 は、パケット 6 の情報をもとに MAILサーバ 2 かどうかの検出を行うルールである。

【0056】検出ルールテーブル 28 は、種類 26 と検出ルール 27 とルール名 14 の関係をまとめた検出ルールリストを記述している。図 4 は、検出ルールリストの構成を示す図である。尚、種類 26 は、マシンが WWWサーバ 1 か MAILサーバ 2 かなどを識別する。

【0057】検出ルールテーブル設定手段 29 は、検出ルールテーブル 28 を設定する。

【0058】検出ルールテーブル取得手段 30 は、検出ルールテーブル 28 から検出ルールリストを取り出す。

【0059】検出ルール実行手段 31 は、パケット 6 と検出ルールリストから検出ルール 27 を実行し、検出ルール 27 からの要求に応じてパケット情報取得・送出手

段23とパケット6のやりとりを行い、検出結果を得る。いずれかのサーバを検出するまで、検出ルールリストにあるすべての検出ルールを実行する。

【0060】IPアドレステーブル変更手段32は、検出結果を元にIPアドレステーブル10を変更する。

【0061】不正侵入判定ルールテーブル変更手段33は、検出結果を元に不正侵入判定ルールテーブル15を変更する。

【0062】次に、動作について説明する。IPアドレステーブル設定手段11により、予めユーザはWWWサーバ1やMAILサーバ2や正常マシン3や不正マシン4などを識別するマシン名8とIPアドレス9の関係をまとめたIPアドレスリストを記述したIPアドレステーブル10を設定しておくことができる。

【0063】また、不正侵入判定ルールテーブル設定手段16により、予めユーザはマシン名8とWWWサーバ用不正侵入判定ルール12やMAILサーバ用不正侵入判定ルール13などを識別するルール名14の関係をまとめたルールリストを記述した不正侵入判定ルールテーブル15を設定しておくことができる。

【0064】そして、ユーザは、検出ルールテーブル設定手段29により、マシンがWWWサーバ1かMAILサーバ2かなどを識別する為の種類26と、WWWサーバ用検出ルール24又はMAILサーバ用検出ルール25の検出ルール27と、WWWサーバ用不正侵入判定ルール12やMAILサーバ用不正侵入判定ルール13などを識別するルール名14を検出ルールテーブル28に設定しておく。

【0065】不正侵入検知システムは、通信手段7によりそのネットワーク5上でデータをのせて流れるパケット6を入手する。

【0066】次に、パケット情報取得・送出手段23により、通信手段7からパケット6を取得する。

【0067】次に、検出ルールテーブル取得手段30により、検出ルールテーブル28から検出ルールリストを全て取り出す。

【0068】次に、検出ルール実行手段31により、パケット6と検出ルールリストから検出ルール27を実行し、検出ルール27からの要求に応じてパケット情報取得・送出手段23とパケット6のやりとりを行い、検出結果を得る。この際に、パケット6は、パケット情報取得・送出手段23と通信手段7を介し、ネットワーク5を経由して対象となるマシンと通信される。

【0069】図5は、WWWサーバ用検出ルールの処理の流れである。S501により、検出ルール実行手段31から実行されたWWWサーバ用検出ルール24の処理が開始される。

【0070】S502により、パケット6の中のIPアドレスを取得する。

【0071】S503により、パケット6の中のIPア

ドレスに対して、PORT番号80の接続要求を送り、検出ルール実行手段31からパケット情報取得・送出手段23を経て通信手段7により実際のパケット6をネットワーク5に送出する。尚、PORT番号80は、WWWサーバのポート番号である。但し、ポート番号を指定せずに、1から順に確認する方法も考えられる。

【0072】S504により、接続結果を確認する。接続成功の場合は、S505を実行する。接続失敗の場合は、S509へ移る。

10 【0073】S505により、同一のIPアドレス及びポート番号に対して改行コードを2個送出し、検出ルール実行手段31からパケット情報取得・送出手段23を経て通信手段7により実際のパケット6をネットワーク5に送出する。

【0074】S506により、ネットワークから取得したパケットを通信手段ならびにパケット情報取得・送出手段、更に検出ルール実行手段を経由してリプライとして受信する。

20 【0075】S507により、リプライの先頭文字が“HTTP/1.0”から始まっているかどうかを比較する。一致した場合は、S508を実行する。不一致の場合は、S509へ移る。

【0076】S508により、相手がWWWサーバであると判定する。尚、HTTPプロトコルにより、WWWサーバがどのように動作することが定義されている。また、“HTTP/1.1”から始まっている場合にも、同様に判定することができる。

【0077】S509により、一連の処理を終了する。

30 【0078】尚、MAILサーバの場合には、PORT番号は、25番となり、HELO testのリプライの先頭文字が“250”から始まっていることにより判定することができる。

【0079】検出結果、新しいIPアドレス9が発見され、更にサーバが検出された場合には、IPアドレステーブル変更手段32によりIPアドレス9と、新たに生成したマシン名8をIPアドレステーブル10に追加する。また、不正侵入判定ルールテーブル変更手段33により、マシン名8とルール名14を不正侵入判定ルールテーブル15に追加する。

40 【0080】次に、パケット情報取得手段17により、通信手段7からパケット6を取得する。この際、通信手段7は自らがネットワーク5に送信したパケット6は渡さずに破棄する。

【0081】次に、IPアドレステーブル取得手段18により、IPアドレステーブル10からパケット6の中に含まれるIPアドレス9に対応するIPアドレスリストを取得する。

50 【0082】次に、不正侵入判定ルールテーブル取得手段19により、不正侵入判定ルールテーブル15からIPアドレスリストに含まれるマシン名8に対応するル

ルテーブルリストを取得する。

【0083】次に、不正侵入判定ルール実行手段20により、ルールテーブルリストからルール名14を取得して実行する。実行結果が不正侵入と判定されたときは、対策実行手段22によりアラーム21を出力する。

【0084】従って、自動的に更新されたIPアドレステーブル10と不正侵入判定ルールテーブル15を用いて侵入検知が実行されることとなる。

【0085】実施の形態2。図6は、実施の形態2における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、IPアドレス設定済検査手段43を備えている。

【0086】IPアドレス設定済検査手段43は、検出ルール実行手段31から与えられたIPアドレス9がIPアドレステーブル10に既に設定されているかどうかを検査して結果を検出ルール実行手段31に渡す。

【0087】動作について説明する。検出ルール実行手段31により検出結果を得る処理までは、実施の形態1における動作と同様である。

【0088】検出結果、新しいIPが発見され、更にサーバが検出された場合には、IPアドレス9を検出ルール実行手段31からIPアドレス設定済検査手段43に渡し、IPアドレス設定済検査手段43により、IPアドレステーブル10に既に設定されているかどうかを検査する。そして、検査結果を検出ルール実行手段31に渡す。

【0089】IPアドレス9が未登録の場合は、IPアドレステーブル変更手段32により、IPアドレス9と新たに生成したマシン名をIPアドレステーブル10に追加する。また、不正侵入判定ルールテーブル変更手段33により、マシン名とルール名を不正侵入判定ルールテーブル15に追加する。

【0090】これ以降の動作は、実施の形態1における動作と同様である。

【0091】本実施の形態では、IPアドレステーブル10にIPアドレス9が重複して設定されることがないので、IPアドレステーブル10が最適な状態に保たれる。

【0092】実施の形態3。図7は、実施の形態3における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、不正侵入判定ルール設定済検査手段44を備えている。

【0093】不正侵入判定ルール設定済検査手段44は、検出ルール実行手段31から与えられたマシン名8とルール名14のペアであるルールリストが不正侵入判定ルールテーブル15に既に設定されているかどうかを検査して結果を検出ルール実行手段31に渡す。

【0094】動作について説明する。検出ルール実行手

段31により検出結果を得る処理までは、実施の形態1における動作と同様である。

【0095】検出結果、新しいIPが発見され、更にサーバが検出された場合には、マシン名8とルール名14を検出ルール実行手段31から不正侵入判定ルール設定済検査手段44に渡し、不正侵入判定ルール設定済検査手段44により、不正侵入判定ルールテーブル15に既に設定されているかどうかを検査する。そして、検査結果を検出ルール実行手段31に渡す。

10 【0096】ルールリストが未登録の場合は、IPアドレステーブル変更手段32により、IPアドレス9と新たに生成したマシン名をIPアドレステーブル10に追加する。また、不正侵入判定ルールテーブル変更手段33によりマシン名とルール名を不正侵入判定ルールテーブル15に追加する。

【0097】これ以降の動作は、実施の形態1における動作と同様である。

【0098】本実施の形態では、不正侵入判定ルールテーブル15にマシン名8とルール名14のペアであるルールリストが重複して設定されることがないので、不正侵入判定ルールテーブル15が最適な状態に保たれる。

【0099】実施の形態4。図8は、実施の形態4における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、IPアドレステーブル再取得手段45、不正侵入判定ルールテーブル再取得手段46、検出ルール再実行手段47、再検出指定手段48を備えている。

20 【0100】IPアドレステーブル再取得手段45は、IPアドレステーブル10からIPアドレスリストを再取得する。

【0101】不正侵入判定ルールテーブル再取得手段46は、不正侵入判定ルールテーブル15からルールリストを再取得する。

【0102】検出ルール再実行手段47は、IPアドレステーブル再取得手段45より与えられるIPアドレスリストと、不正侵入判定ルールテーブル再取得手段46より与えられるルールリストと、検出ルールテーブル取得手段30より得られる検出ルールリストを用いて、検出ルール実行手段31に再実行させる。

40 【0103】再検出指定手段48は、検出ルール再実行手段47に実行を指示する。

【0104】動作について説明する。ユーザは、任意の時点で再検出指定手段48により検出ルール再実行手段47に実行を指示することができる。

【0105】IPアドレステーブル再取得手段45は、IPアドレステーブル10からIPアドレスリストを再取得し、不正侵入判定ルールテーブル再取得手段46は、不正侵入判定ルールテーブル15からルールリストを再取得し、更に、検出ルールテーブル取得手段30は、検出ルールリストを取得する。

【0106】検出ルール再実行手段47は、ルールリスト中のルール名14に対応する検出ルールリスト中の検出ルール27と、ルールリスト中のマシン名8に対応するIPアドレステーブル10中のIPアドレス9を取得し、これを検出ルール実行手段31に渡して再実行させる。

【0107】次に、検出ルール実行手段31により、検出ルール27を実行し、検出ルール27からの要求に応じてパケット情報取得・送出手段23とパケット6のやりとりを行い検出結果を得る。

【0108】この際にパケット6は、パケット情報取得・送出手段23と通信手段7を介し、ネットワーク5を経由して対象となるマシンと通信される。

【0109】検出結果、サーバが検出されなかった場合には、不正侵入判定ルールテーブル変更手段33によりマシン名8とルール名14を不正侵入判定ルールテーブル15から削除する。また、IPアドレス9が検出されなかった場合には、IPアドレステーブル変更手段32によりIPアドレス9とマシン名8をIPアドレステーブル10から削除し、不正侵入判定ルールテーブル変更手段33によりマシン名8とルール名14を不正侵入判定ルールテーブル15から削除する。

【0110】次に、パケット情報取得手段17により、通信手段7からパケット6を取得する。この際、通信手段7は自らがネットワーク5に送信したパケット6は渡さずに破棄する。

【0111】次に、IPアドレステーブル取得手段18により、IPアドレステーブル10からパケット6の中に含まれるIPアドレス9に対応するIPアドレスリストを取得する。

【0112】次に、不正侵入判定ルールテーブル取得手段19により、不正侵入判定ルールテーブル15からIPアドレスリストに含まれるマシン名8に対応するルールテーブルリストを取得する。

【0113】次に、不正侵入判定ルール実行手段20によりルールテーブルリストからルール名14を取得して実行する。実行結果が不正侵入と判定された時は対策実行手段22によりアラーム21を出力する。

【0114】従って、再検出の指定のみで自動的に更新されたIPアドレステーブル10と不正侵入判定ルールテーブル15を用いて侵入検知が実行されることとなる。

【0115】実施の形態5. 図9は、実施の形態5における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、再検出指定手段48、アラーム検出手段49を備えている。

【0116】アラーム検出手段49は、アラーム21の出力を検出して、再検出指定手段48に再検出を指示する。

【0117】本実施の形態では、ユーザが再検出指定手段48を操作して検出ルール再実行手段47に再実行を指示するかわりに、アラーム検出手段49によりアラーム21の発生を検出し、再検出指定手段48に再実行を自動的に指示する。

【0118】従って、何らかの異常が発生または設定の更新が必要と考えられる場合に、迅速に対応することが可能となる。

【0119】実施の形態6. 図10は、実施の形態6における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、設定時パスワード入力手段51、起動時パスワード入力手段52、実行時パスワード保存手段53、暗号済検出ルールテーブル54、検出ルールテーブル暗号設定手段55、検出ルールテーブル復号取得手段56、暗号済IPアドレステーブル57、IPアドレステーブル暗号設定手段58、IPアドレステーブル復号取得手段59、IPアドレステーブル暗号変更手段60、暗号済不正侵入判定ルールテーブル61、不正侵入判定ルールテーブル暗号設定手段62、不正侵入判定ルールテーブル復号取得手段63、不正侵入判定ルールテーブル暗号変更手段64を備えている。

【0120】本実施の形態におけるパスワード50は、管理者しか知り得ぬパスワードである。

【0121】設定時パスワード入力手段51は、設定時にパスワード50を入力する。

【0122】起動時パスワード入力手段52は、起動時にパスワード50を入力する。

【0123】実行時パスワード保存手段53は、起動時パスワード入力手段52により入力されたパスワード50を実行時にのみ保存する。

【0124】暗号済検出ルールテーブル54は、パスワード50により暗号化された検出ルールリストを格納する。

【0125】検出ルールテーブル暗号設定手段55は、パスワード50により暗号化して暗号済検出ルールテーブル54を設定する。

【0126】検出ルールテーブル復号取得手段56は、暗号済検出ルールテーブル54よりパスワード50にて復号した検出ルールリストを取得する。

【0127】暗号済IPアドレステーブル57は、パスワード50により暗号化されたIPアドレスリストを格納する。

【0128】IPアドレステーブル暗号設定手段58は、パスワード50により暗号化して暗号済IPアドレステーブル57を設定する。

【0129】IPアドレステーブル復号取得手段59は、暗号済IPアドレステーブル57よりパスワード50にて復号したIPアドレスリストを取得する。

【0130】IPアドレステーブル暗号変更手段60

は、パスワード 50 により復号し再度暗号化して暗号済 I P アドレステーブル 57 を変更する。

【0131】暗号済不正侵入判定ルールテーブル 61 は、パスワード 50 により暗号化されたルールリストを格納する。

【0132】不正侵入判定ルールテーブル暗号設定手段 62 は、パスワード 50 により暗号化して暗号済不正侵入判定ルールテーブル 61 を設定する。

【0133】不正侵入判定ルールテーブル復号取得手段 63 は、暗号済不正侵入判定ルールテーブル 61 よりパスワード 50 にて復号したルールリストを取得する。

【0134】不正侵入判定ルールテーブル暗号変更手段 64 は、パスワード 50 により復号し、再度暗号化して暗号済不正侵入判定ルールテーブル 61 を変更する。

【0135】動作について説明する。システム起動時に、管理者は、管理者しか知り得ぬパスワード 50 を、起動時パスワード入力手段 52 により入力し、実行時パスワード保存手段 53 により実行中のみ保存する。

【0136】暗号済検出ルールテーブル 54 には、パスワード 50 により暗号化された検出ルールリストが格納される。暗号済検出ルールテーブル 54 を設定する場合には、検出ルールテーブル暗号設定手段 55 によりパスワード 50 にて暗号化する。暗号済検出ルールテーブル 54 により検出ルールリストを取得する場合には、検出ルールテーブル復号取得手段 56 によりパスワード 50 にて復号する。

【0137】暗号済 I P アドレステーブル 57 には、パスワード 50 により暗号化された I P アドレスリストが格納される。暗号済 I P アドレステーブル 57 を設定する場合には、I P アドレステーブル暗号設定手段 58 によりパスワード 50 にて暗号化する。暗号済 I P アドレステーブル 57 より I P アドレスリストを取得する場合には、I P アドレステーブル復号取得手段 59 によりパスワード 50 にて復号する。暗号済 I P アドレステーブル 57 を変更する場合には、I P アドレステーブル暗号変更手段 60 によりパスワード 50 にて復号し再度暗号化する。

【0138】暗号済不正侵入判定ルールテーブル 61 には、パスワード 50 により暗号化されたルールリストが格納される。暗号済不正侵入判定ルールテーブル 61 を設定する場合には、不正侵入判定ルールテーブル暗号設定手段 62 によりパスワード 50 にて暗号化する。暗号済不正侵入判定ルールテーブル 61 よりルールリストを取得する場合には、不正侵入判定ルールテーブル復号取得手段 63 によりパスワード 50 にて復号する。暗号済不正侵入判定ルールテーブル 61 を変更する場合には、不正侵入判定ルールテーブル暗号変更手段 64 によりパスワード 50 にて復号し再度暗号化する。

【0139】この他の動作は、実施の形態 1 と同様である。

【0140】従って、管理者と当侵入検知システム以外の者により、設定情報が改ざんされることを防止できる。

【0141】実施の形態 7. 図 11 は、実施の形態 7 における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、検出ルールテーブル 28 及び I P アドレステーブル 10 及び検出ルールテーブル 28 の変更履歴を格納する履歴テーブル 65 と、検出ルールテーブル 28 及び I P アドレステーブル 10 及び検出ルールテーブル 28 の変更履歴を履歴テーブル 65 に格納するテーブル変更保存手段 66 を備えている。

【0142】また、図 12 は、この発明における履歴テーブルの構成の一例である。

【0143】本実施の形態では、検出ルールテーブル設定手段により、検出ルールテーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。不正侵入判定ルールテーブル設定手段により、ルールテーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。不正侵入判定ルールテーブル変更手段により、ルールテーブルを変更する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。I P アドレステーブル設定手段により、I P アドレステーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。I P アドレス不正侵入判定ルールテーブル変更手段により、I P アドレスルールテーブルを変更する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。

【0144】この他の動作は、実施の形態 1 と同様である。

【0145】従って、ユーザによる設定変更および当侵入検知システムによる設定変更を後で確認することが可能となり管理負荷の低減と利便性が向上する。

【0146】実施の形態 8. 図 13 は、実施の形態 8 における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、通信手段 7 より得られるパケット 6 を保存しておくパケット保存手段 67 と、パケット保存手段 67 に保存されているパケット 6 を再生するパケット再生手段 68 と、パケット再生手段 68 にパケット 6 の再生を指示するパケット再生指示手段 69 を備えている。尚、ここで再生するとは、保存されているパケットを通信手段によりネットワークへ送出することである。

【0147】動作について説明する。本実施の形態では、パケット保存手段 67 により、通信手段 7 より得られるパケット 6 を保存し、パケット再生手段 68 により、パケット保存手段 67 に保存されているパケット 6 を再生する。ユーザーは、パケット再生指示手段 69 により、パケット再生手段 68 にパケット 6 の再生を指示する。

【0148】この他の動作は、実施の形態1と同様である。

【0149】従って、ユーザーの指定した時に、それまで保存しておいたパケット6の情報をもとに設定更新を実行させることができるので、企業等においては、ネットワーク5の混雑する昼間はパケット6を保存しておき、適当な時に設定更新作業を実施させることが可能である。

【0150】実施の形態9. 図14は、実施の形態9における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態8の侵入検知システムの構成に加えて、現在の日時を取得する日時取得手段70と、パケット再生指示を出す日時を記述した再生スケジュール71と、現在の日時と再生スケジュール71を比較して指定された日時にパケット再生指示を出す指定日時パケット再生指示手段72を備えている。

【0151】動作について説明する。本実施の形態では、指定日時パケット再生指示手段72が、日時取得手段70により現在の日時を取得し、再生スケジュール71に記述されたパケット再生指示を出す日時と比較して、指定された日時にパケット再生指示をパケット再生手段68に出す。

【0152】この他の動作は、実施の形態8と同様である。

【0153】従って、深夜等の利用者の少ない時間帯に設定更新作業を自動で実施させることが可能である。また、定期的に設定更新作業を実施させることも可能である。

【0154】実施の形態10. 図15は、実施の形態10における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態8の侵入検知システムの構成に加えて、システムの負荷状況を取得する負荷取得手段73と、パケット再生指示を出すことのできる負荷情報を記述した再生可能負荷情報74と、現在の負荷情報と再生可能負荷情報とを比較して可能な負荷状況であればパケット再生指示を出す低負荷時パケット再生指示手段75を備えている。

【0155】動作について説明する。低負荷時パケット再生指示手段75が、負荷取得手段73によりシステムの負荷状況を取得し、再生可能負荷情報74に記述されたパケット再生指示を出すことのできる負荷情報と比較して、可能な負荷状況であればパケット再生指示をパケット再生手段68に出す。

【0156】この他の動作は、実施の形態8と同様である。なお、負荷取得手段73は一定時間プログラムをループでまわし、その実行回数をカウントするなどの方法により実現される。

【0157】従って、システムの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、侵入検知機能のスループットを下げることが防げる。

【0158】実施の形態11. 図16は、実施の形態11における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態8の侵入検知システムの構成に加えて、パケット保存手段67からパケット6の流通量を取得するパケット流通量取得手段76と、パケット再生指示を出すことのできるパケット流通量を記述した再生可能流通量情報77と、現在のパケット流通量と再生可能流通量情報77とを比較して可能な流通量であればパケット再生指示を出す低ネットワーク負荷時パケット再生指示手段78を備えている。

【0159】動作について説明する。低ネットワーク負荷時パケット再生指示手段78が、パケット流通量取得手段76によりパケット6の流通量を取得し、再生可能流通量情報77に記述されたパケット再生指示を出すことのできるパケット流通量と比較して、可能な流通量であればパケット再生指示をパケット再生手段68に出す。

【0160】この他の動作は、実施の形態8と同様である。

【0161】従って、ネットワークの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、ネットワークに繋がれた他の機器への影響を減らすことが可能である。

【0162】尚、上記の説明では、ネットワークにWWWサーバやMAILサーバがある場合について述べたが、その他のサーバに利用することも出来る。

【0163】

【発明の効果】本発明においては、自動的に更新されたIPアドレステーブル10と不正侵入判定ルールテーブル15を用いて侵入検知が実行されることとなる。

【0164】また、この発明は、IPアドレステーブル10にIPアドレス9が重複して設定されることがないので、IPアドレステーブル10が最適な状態に保たれる。

【0165】また、この発明は、不正侵入判定ルールテーブル15にマシン名8とルール名14のペアであるルールリストが重複して設定されることがないので、不正侵入判定ルールテーブル15が最適な状態に保たれる。

【0166】また、この発明は、再検出の指定のみで自動的に更新されたIPアドレステーブル10と不正侵入判定ルールテーブル15を用いて侵入検知が実行されることとなる。

【0167】また、この発明は、何らかの異常が発生または設定の更新が必要と考えられる場合に、迅速に対応することが可能となる。

【0168】また、この発明は、管理者と当侵入検知システム以外の者により、設定情報が改ざんされることを防止できる。

【0169】また、この発明は、ユーザによる設定変更および当侵入検知システムによる設定変更を後で確認す

ることが可能となり管理負荷の低減と利便性が向上する。

【0170】また、この発明は、ユーザーの指定した時に、それまで保存しておいたパケット6の情報をもとに設定更新を実行させることができるので、企業等においては、ネットワーク5の混雑する昼間はパケット6を保存しておき、適当な時に設定更新作業を実施させることが可能である。

【0171】また、この発明は、深夜等の利用者の少ない時間帯に設定更新作業を自動で実施させることが可能である。また、定期的に設定更新作業を実施させることも可能である。

【0172】また、この発明は、システムの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、侵入検知機能のスループットを下げる事が防げる。

【0173】また、この発明は、ネットワークの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、ネットワークに繋がれた他の機器への影響を減らすことが可能である。

【図面の簡単な説明】

【図1】 実施の形態1における侵入検知システムを示す図である。

【図2】 IPアドレステーブルの構成を示す図である。

【図3】 ルールテーブルの構成を示す図である。

【図4】 検出ルールリストの構成を示す図である。

【図5】 WWWサーバ用検出ルールの処理の流れを示す図である。

【図6】 実施の形態2における侵入検知システムを示す図である。

【図7】 実施の形態3における侵入検知システムを示す図である。

【図8】 実施の形態4における侵入検知システムを示す図である。

【図9】 実施の形態5における侵入検知システムを示す図である。

【図10】 実施の形態6における侵入検知システムを示す図である。

【図11】 実施の形態7における侵入検知システムを示す図である。

【図12】 この発明における履歴テーブルの構成の一例を示す図である。

【図13】 実施の形態8における侵入検知システムを示す図である。

【図14】 実施の形態9における侵入検知システムを示す図である。

【図15】 実施の形態10における侵入検知システム

を示す図である。

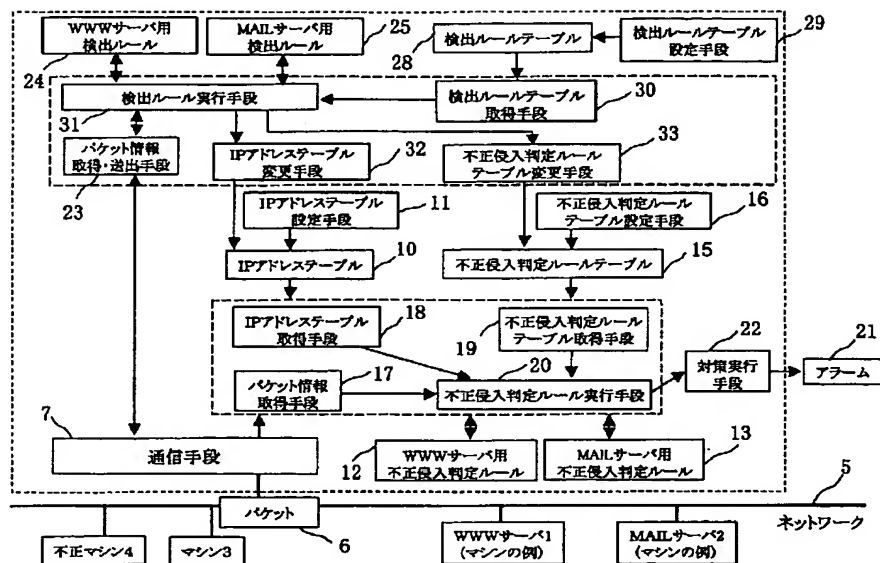
【図16】 実施の形態11における侵入検知システムを示す図である。

【図17】 従来の侵入検知システムを示す図である。

【符号の説明】

1 WWWサーバ、2 MAILサーバ、3 正常マシン、4 不正マシン、5 ネットワーク、6 パケット、7 通信手段、8 マシン名、9 IPアドレス、10 IPアドレステーブル、11 IPアドレステーブル設定手段、12 WWWサーバ用不正侵入判定ルール、13 MAILサーバ用不正侵入判定ルール、14 不正侵入判定ルール名、15 不正侵入判定ルールテーブル、16 不正侵入判定ルールテーブル設定手段、17 パケット情報取得手段、18 IPアドレステーブル取得手段、19 不正侵入判定ルールテーブル取得手段、20 不正侵入判定ルール実行手段、21 アラーム、22 対策実行手段、23 パケット情報取得・送出手段、24 WWWサーバ用検出ルール、25 MAILサーバ用検出ルール、26 種類、27 検出ルール、28 検出ルールテーブル、29 検出ルールテーブル設定手段、30 検出ルールテーブル取得手段、31 検出ルール実行手段、32 IPアドレステーブル変更手段、33 不正侵入判定ルールテーブル変更手段、43 IPアドレス設定済検査手段、44 不正侵入判定ルール設定済検査手段、45 IPアドレステーブル再取得手段、46 不正侵入判定ルールテーブル再取得手段、47 検出ルール再実行手段、48 再検出指定手段、49 アラーム検出手段、51 設定時パスワード入力手段、52 起動時パスワード入力手段、53 実行時パスワード保存手段、54 暗号済検出ルールテーブル、55 検出ルールテーブル暗号設定手段、56 検出ルールテーブル復号取得手段、57 暗号済IPアドレステーブル、58 IPアドレステーブル暗号設定手段、59 IPアドレステーブル復号取得手段、60 IPアドレステーブル暗号変更手段、61 暗号済不正侵入判定ルールテーブル、62 不正侵入判定ルールテーブル暗号設定手段、63 不正侵入判定ルールテーブル復号取得手段、64 不正侵入判定ルールテーブル暗号変更手段、65 履歴テーブル、66 テーブル変更保存手段、67 パケット保存手段、68 パケット再生手段、69 パケット再生指示手段、70 日時取得手段、71 再生スケジュール、72 指定日時パケット再生指示手段、73 負荷取得手段、74 再生可能負荷情報、75 低負荷時パケット再生指示手段、76 パケット流通量取得手段、77 再生可能流通量情報、78 低ネットワーク負荷時パケット再生指示手段。

【図 1】



【図 2】

IPアドレステーブル		9
マシン名 (マシンの識別情報の例)	IPアドレス	8
WWW_1	10.0.0.3	
MAIL_2	10.0.0.4	8

【図 3】

不正侵入判定ルールテーブル		14
マシン名 (マシンの識別情報の例)	不正侵入判定ルール名 (不正侵入判定ルールの識別情報の例)	8
WWW_1	WWWサーバ用不正侵入判定ルール	
MAIL_2	MAILサーバ用不正侵入判定ルール	8

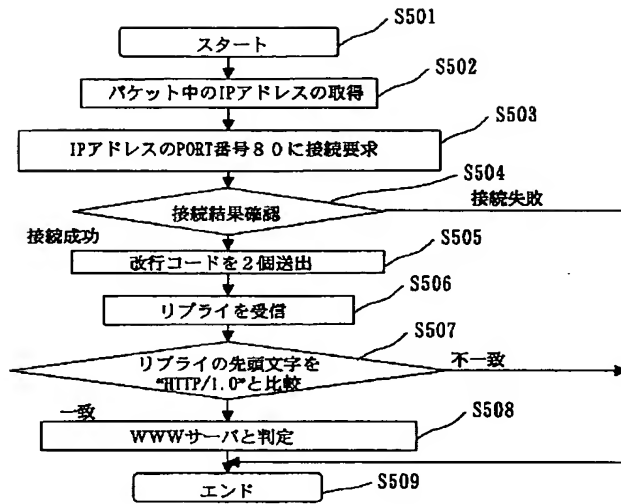
【図 4】

検出ルールリスト			26	27	14
サーバの種類	検出ルール		不正侵入判定ルール		
WWWサーバ	WWWサーバ用検出ルール		WWWサーバ用ルール		
MAILサーバ	MAILサーバ用検出ルール		MAILサーバ用ルール		

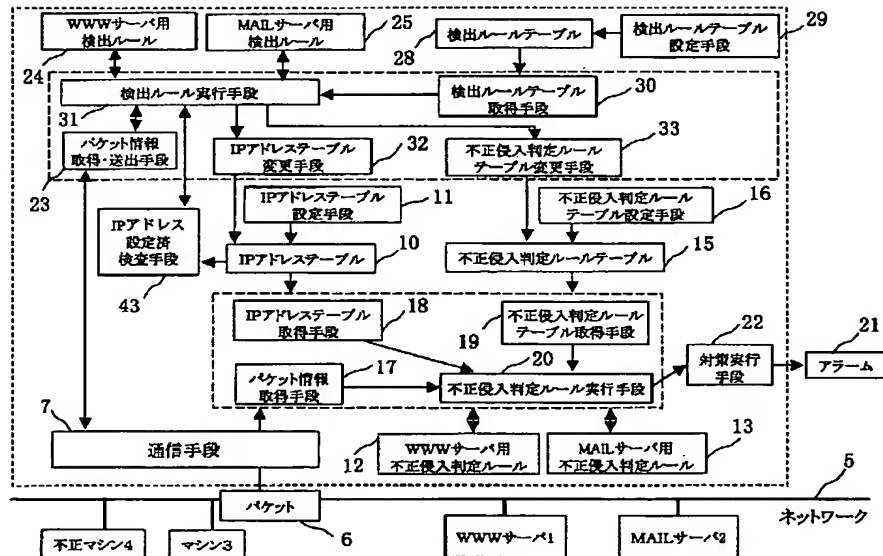
【図 12】

履歴テーブル		
操作手段名	操作対象名	操作内容
ルールテーブル設定手段	ルールテーブル	追加 (マシン名: WWW1、ルール名: WWWサーバ用ルール)
IPアドレステーブル設定手段	IPアドレステーブル	追加 (マシン名: WWW1、IPアドレス: 10.0.0.3)

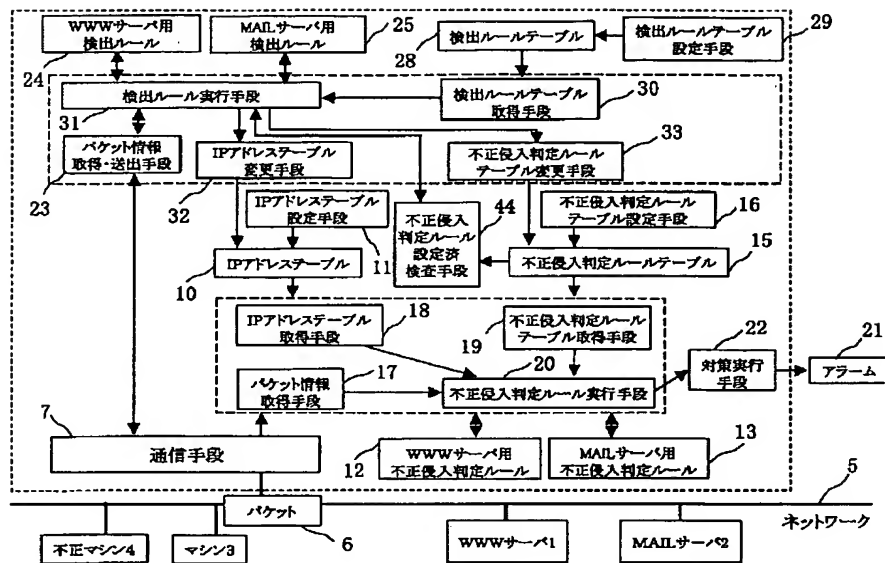
【図5】



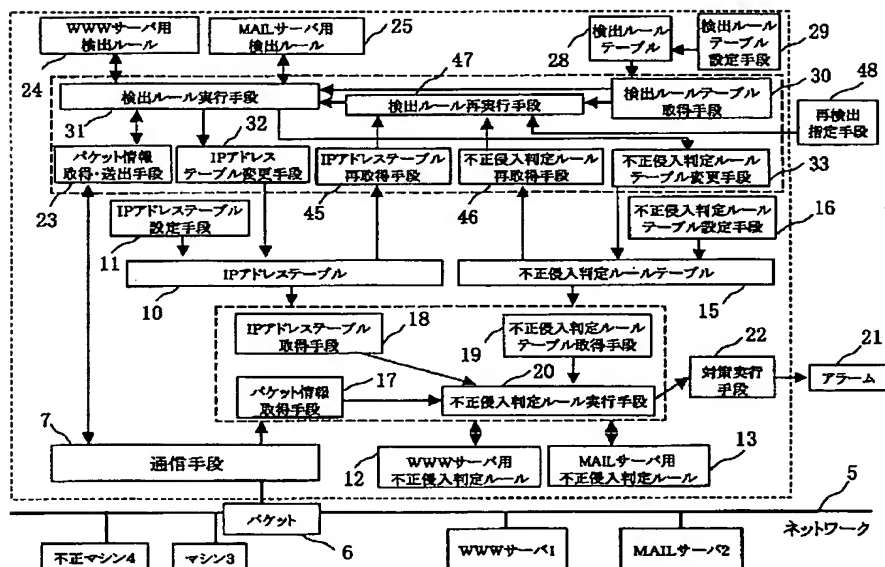
【図6】



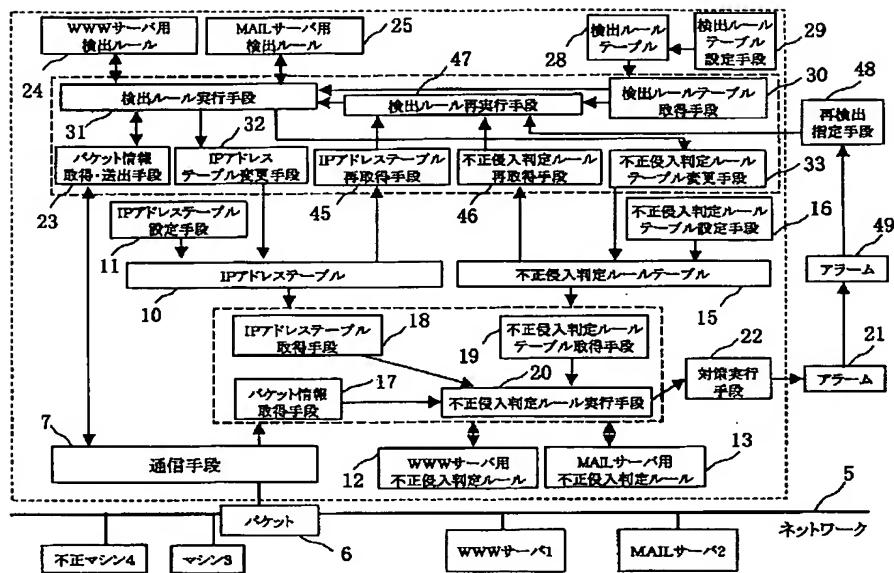
【図7】



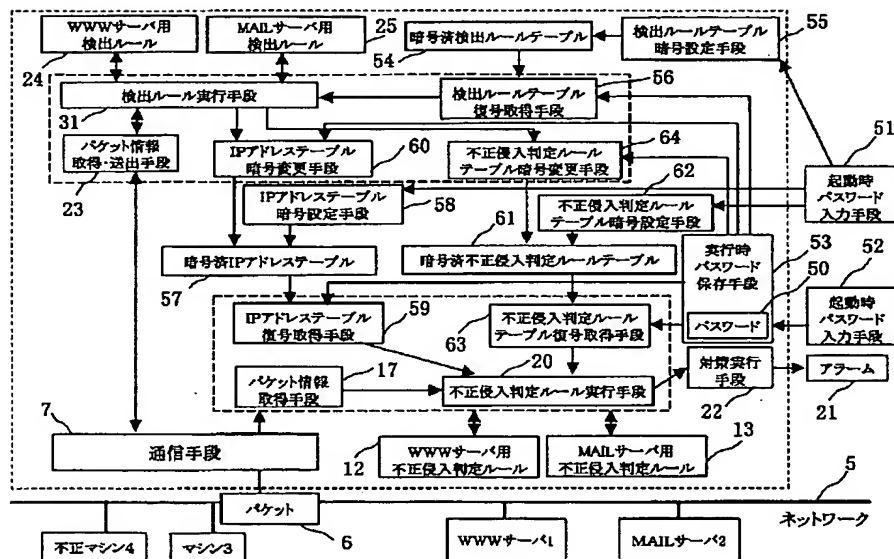
【図8】



【図9】



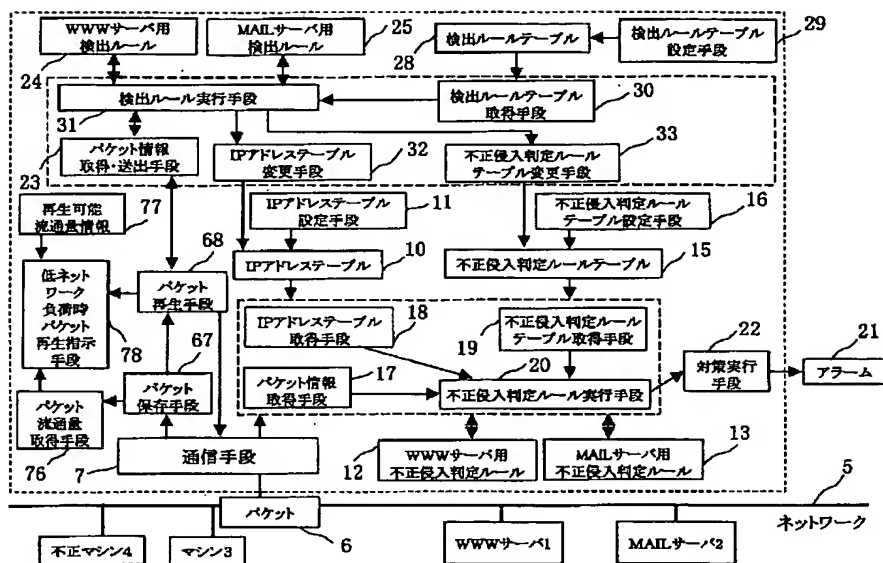
【図10】



[illegible][illegible]

[illegible][illegible]

【図16】



【図17】

